Information and Communications Technology Policy

Policy name: Information and Communications Technology Policy

Approved: 25th November 2016
Revision 1 approved 10th March 2017
Revision 2 approved
Revision 3 approved by Trinity Academic Council 13th May 2020
Revision 4 approved by RIAM Governing Body 11th July 2024

Table of Contents

1. Context

1.1 Information is a critical asset of the Royal Irish Academy of Music (hereinafter referred to as RIAM or the Academy). Accurate, timely, relevant and properly protected information is essential for the success of RIAM's academic and administrative activities. RIAM is committed to ensuring that all access to, use of, and processing of this information is performed in a secure manner and that best practice standards are adopted during all information and communications technology (ICT) operations.

1.2 Technological information systems play a major role in supporting the day-to-day activities of RIAM. These information systems comprise all infrastructure, networks, hardware, databases and other software applications, which are used to manipulate, process, transport, or store information owned by RIAM. These include but are not limited to: communication systems (including telephone, facsimile, email, broadband and web services).

1.3 Information that RIAM or its contractual agents use in the course of conducting its business is an institutional resource. It is responsibility of all RIAM's employees, contractors, subcontractors, vendors, suppliers, and students to comply with this policy. Although individuals and departments may have responsibility for creating and maintaining portions of RIAM information and records, the institution itself retains ownership of, and responsibility for this information.

1.4 RIAM recognises that failure to implement best practice standards and adequate security controls could potentially lead to (i) financial loss, (ii) irretrievable loss of important RIAM data, (iii) damage to RIAM's reputation, or (iv) legal consequences and GDPR. Thus RIAM has put in place measures to minimise the risk to RIAM from unauthorised modification, destruction or disclosure of data, whether accidental or deliberate.

2. Purpose

The purpose of this policy is to define guidelines for the implementation of information security controls within RIAM and enable the institution to fulfil its responsibilities with regard to information security and ensure that a high level of service is provided to staff, students and other stakeholders.

The objective is to provide all information assets of RIAM with:

Confidentiality: To ensure all information is accessible to only those authorised to have access.
Integrity: To safeguard the accuracy and completeness of information and processing methods.
Availability: To ensure that authorised users have access to information and the supporting processes, systems and networks when required.

3. Scope

3.1 The scope of this policy encompasses all possible uses of RIAM's information and information assets, as well as all security aspects (human, logical, physical, regulatory, etc.).

3.2 The following non-exclusive list of in scope assets covered by this policy is as follows:

information assets, software assets, physical assets, communication and computing services including but not limited to; Internet, Wi-Fi, email, voicemail, cloud-based assets, file-sharing, printing, storage and backups.

3.3 The scope also includes the physical protection of all RIAM ICT assets.

4. Benefits

4.1 This policy provides a framework in which security threats to RIAM information and communication systems can be identified and managed on a risk basis.

4.2 It also establishes the terms of reference, which ensure uniform implementation of information and communication security controls throughout RIAM.

5. Principles

5.1 RIAM undertakes to ensure that the institution's information in any form, and related assets are created, used, communicated and maintained in a secure environment.

5.2 All RIAM information will be kept accurate and up-to-date and available for authorised use.

5.3 All RIAM computing facilities, programs, data, network and equipment will be monitored and kept adequately protected against loss, misuse or abuse.

5.4 Security measures must be implemented by all RIAM service users as part of the effective operation and support of ICT across the organisation and when used to communicate with the outside world.

5.5 All RIAM users must understand their own responsibilities for respecting the rights of individuals and protecting the confidentiality and integrity of the data they handle.

5.6 All RIAM service users must be aware of and fully comply with the relevant Irish and European Community legislation i.e. Data Protection Act 2018 and General Data Protection Regulation (GDPR) and later amendments.

5.7 All RIAM service users must be aware of and fully comply with this ICT policy and the relevant supporting policies and procedures.

5.8 Successful implementation of this strategy can only be achieved if all service users cooperate by observing the highest standards of ethical, personal and professional conduct.

6. Policy

6.1 Acceptable Usage

RIAM encourages all staff, students and external parties to apply a professional attitude towards their individual working environment, including the use of RIAM ICT resources. Staff, students and external parties are responsible for their individual user accounts and password details**.**

(i) Reasonable care must be taken to ensure that the use of resources does not reduce the level of integrity, performance or reliability of RIAM ICT resources (e.g. broadband, mobile print), or result in a denial of service to others. Staff, Students and external parties should not jeopardise RIAM's business information, confidential information or intellectual property through the use of social media, internet file sharing or internet file storage sites.

(ii) Do not bring RIAM into disrepute

(iii) Do not defame or disparage RIAM or other staff, students, and/or external parties

(iv) Do not harass or bully another individual or group in any way

(v) Do not unlawfully discriminate against another individual or group. It is against the law to discriminate against another on grounds of gender, marital status, family status, sexual orientation, religion, age, disability, race or membership of an ethnic minority.

(vi) Do not represent yourself as another person

(vii) Do not breach data protection legislation (for example, never disclose personal information

6.1.1 Email Service

RIAM recognizes that email is a fast, reliable and cost-effective method of delivering messages and documents and, in view of this, encourages its use. RIAM aims to provide an email facility that is capable of meeting the business needs of each stakeholder. However, this policy is not exhaustive. In situations that are not expressly governed therein, service users must ensure that their use of e-mail is at all times appropriate and consistent with their responsibilities towards RIAM. In case of any doubt, they should consult with their manager or the HR department.

(i) Service users are required to behave in a professional and responsible manner whether accessing email from within the Academy or using RIAM resources over the Internet, which includes professional and respectful communication methods within emails. RIAM recommends:

- Use standard fonts (such as Calibri or Arial), appropriate colours, and font sizes for official RIAM emails.
- Avoid excessive use of bold or italics within a single email.
- Title your email so the recipient knows the purpose of the message.
- Sign off with a professional closing (e.g., “Kind regards” or “Thank you”).
- Use “Reply all” sparingly to avoid cluttering inboxes.
- Keep emails direct and concise.
- Maintain a professional and respectful tone.
- Avoid capitalising words or using offensive or inappropriate language.
- If emailing someone for the first time, introduce yourself briefly and provide context for your email.

Consider using a share link from HEAnet Filesender, SharePoint or OneDrive rather than attaching a document, particularly for confidential documents.

(ii) All emails sent will be identified by the username as coming from RIAM and service users should take care to uphold RIAM corporate values and good reputation. Therefore, users should actively seek to use the most appropriate means of communication.

(iii) Service users must adhere to laws on defamation, copyright, obscenity, fraud, discrimination and data protection when using email to communicate.

(iv) RIAM is not liable for any information sent by a user of the system in the event that the user chooses to send information in violation of this policy.

(v) Commercial use, which is not connected to or approved by RIAM, is strictly prohibited.

(vi) Email is a business tool which should only be used for reasonable purposes. Reasonable use is defined as use that does not impair the system or impact negatively on user's job performance or on the work or reputation of the institution.

(vii) Reasonable personal use is permitted, however RIAM strongly recommends using RIAM email for business use only. Please note that all business communication must be conducted through RIAM email or Teams.

(viii) Service users are reminded that all information on the email system is the property of RIAM and may be monitored. While RIAM does not routinely monitor the content of e-mail messages, it may, for computer maintenance and other purposes, analyse e-mails individually or collectively. Circumstances giving rise to such analysis include, but are not limited to:

- investigations triggered by indications of misconduct;
- the detection of computer viruses;
- monitoring proper use;
- the location of information required for business purposes;
- responding to legal or regulatory requirements;
- fulfilment of obligations to customers, clients, third parties and relevant regulatory authorities.

(ix) The only personal email data that may be held in RIAM accounts is email information relating to RIAM business.

(x) In particular, staff members who also have responsibility for communications on behalf or other organisations, may not store other email data with RIAM email data; and, in general, unless explicit permission has been obtained from the Director, may not store email data relating to these other organisations on systems provided by the RIAM e.g. PCs, laptops, mobile phones, databases, etc.

(xi) It is acceptable to open emails and attachments from trusted sources. However if an email is received from an unrecognised sender or with a non-standard attachment type, the recipient should not open the email but instead contact the ICT Manager immediately at tech@riam.ie.

(xii) Service users should be alert to phishing attempts and should examine carefully any messages from outside the organisation purporting to come from members of the Senior Management or Finance Office Teams before responding, opening attachments, or clicking on any links. Tell-tale signs include generic text, incorrect capitalisation, and missing names or signatures. Any phishing attempts should be reported to the ICT Manager at tech@riam.ie.

(xiii) It is acceptable to open attachment using standard file formats e.g. MS Word, MS Excel, etc. In order to maintain the integrity of ICT systems, staff members are urged to contact the ICT Manager should it be necessary to open any non-standard file formats.

(xiv) It is inappropriate use of email to:

- use someone else’s ID to send mail;
- use e-mail to circulate inappropriate electronic mail, joke mail or chain letters, internally or externally;
- use e-mail to harass or intimidate another person, broadcast unsolicited messages, or send unwanted mail;
- forward an email message where permission has been withheld by the originator;
- forward electronic mail messages with attachments to large internal mail distribution lists without prior authorisation from RIAM ICT;
- remove any copyright, trademark or other proprietary rights notices contained in or on the email message;
- use BCC to address recipients inappropriately;
- communicate to another in any manner that could cause him or her distress, embarrassment, or cause unwarranted attention. There must be no personal attacks, inclusive of those based on gender, race, national origin, ethnicity, religion, disability, sexual orientation, or membership of the traveller community;
- use e-mail, or other system resources, to gain access to, or possession of, pornographic materials;
- accept/open electronic mail messages that might be harmful to RIAM’s computing resources, or to information stored thereon;
- use vulgar, abusive, or hateful language;
- save, download, transmit or purposely view sexual, pornographic, racist, profane or other offensive material;
- download software, graphical or other forms of information for personal use;
- produce advertising or listings for personal benefit;
- use the e-mail system to send mail that may be damaging to the organisation’s corporate image;

- engage in any activity that is in competition with the commercial interests of the organisation;

- subscribe to any contracts, unless authorised to do so within the terms of the organisation's policy on purchasing;

- accept any material by e-mail that may give rise to a breach of the intellectual property rights of any outside party;

- use RIAM resources to participate in an unsolicited advertising ("spamming") campaign

- engage in any other activity that does not comply with the principles presented above.

(xv) RIAM is committed to protecting its service users from the effects of inappropriate use of e-mail by others. If service users receive any offensive, unpleasant, harassing, or intimidating messages via e-mail, they should report this immediately. It is important that the sources of such e-mails are traced as quickly as possible. The message should be printed and kept for investigative purposes.

(xvi) If any breach of this e-mail policy is observed and proven, then disciplinary action (for staff, up to and including dismissal) may be taken.

6.1.2 Direct Marketing

(i) It is RIAM's intention to continue to use email to provide information, newsletters, updates, notices of events, invitations to concerts, solicitations for donations, etc., to its large and diverse community of stakeholders.

(ii) In compliance with GDPR when collecting personal information, including email addresses, RIAM must advise individuals what information is being collected, for what purposes, how long it will be retained, and how it can be corrected, updated or deleted by the individual.

(iii) Personal information collected for reasonable business purposes (e.g. processing an application for RIAM Exams) that a person requests (and consents to) does not require additional explicit consent. Individuals providing information on behalf of others must confirm that appropriate consent has been obtained.

(iv) Personal information collected for communications or marketing purposes, outside of the normal RIAM reasonable business processes, requires explicit (opt-in) consent from individuals for each specific communications or marketing purpose. RIAM must carefully define these purposes and ensure that communications to individuals are consistent with the purposes for which explicit opt-in consent has been obtained. RIAM must record these consents.

(v) RIAM has a large set of existing collected email addresses. It has been careful to ensure that implicit consent was obtained for the appropriate purposes, but must now establish a process to update these consents to explicit opt in consents.

(vi) RIAM will, over time, email all the individuals whose email addresses are on file, and

- advise them of the purposes for which email addresses are currently being used

- advise them that email addresses currently on file will be deleted after the current year or until they cease to be of administrative use (ref RIAM Records Retention Policy)

- invite them to opt-in to one or more of a range of defined RIAM email communications

- Advise of ability to opt-out

- These consents will be recorded and will be used to ensure that thereafter the email addresses will only be used for the agreed purposes.

- The wording of the email that will be sent out to stakeholders advising them of their rights and protection under GDPR will be approved by the ICT Steering Committee.

- RIAM will delete all records of those individuals who have not provided their explicit consent for the various purposes at the end of the Initial Retention Period.

- Users are expected to act ethically and responsibly in their use of emails for direct marketing purposes and to comply with the relevant national legislation available from the Data Protection Commission website.

6.1.4 Internet

RIAM recognises that the Internet is an important business resource and aims to provide access to the Internet for its entire staff and student community subject to acceptance of this policy and abiding by its contents.

(i) Internet access for business purposes in RIAM is available only via the RIAM infrastructure. Users wishing to connect a non-RIAM machine to the Internet via the RIAM business network must seek authorisation from the ICT Manager at tech@riam.ie (ref Bring Your Own Device and Use of Facilities policy).

(ii) RIAM third level students and guests may access Internet through a secure Wi-Fi system.

(iii) All devices connected to the Internet must be equipped with the latest versions of anti-virus software. All forms of data received over the Internet should be immediately checked for viruses. All forms of data transmitted from RIAM over the Internet should be virus checked. All security incidents involving Internet access must be reported to the ICT Manager.

(iv) Reasonable use is defined as use that does not impair RIAM systems or impact negatively on the service user's job performance or on the work or reputation of RIAM.

(v) Commercial use, which is not connected to or approved by RIAM, is strictly prohibited and will result in disciplinary procedures.

(vi) Service users are expected to act ethically and responsibly in their use of the Internet and to comply with the relevant national legislation, RIAM's regulations and codes of practice.

(vii) Software copyrights and license conditions must be observed. Only licensed files or software may be downloaded from the Internet.

(viii) Reasonable personal use is permitted. However, service users are reminded that all information stored on RIAM systems is the property of the Academy and can be monitored.

(ix) Due to the recent prevalence of threats such as viruses and spyware, service users are asked to be particularly vigilant when using the Internet. Non-reputable sites such as those offering free music or programme downloads must not be used.

(x) RIAM has restricted access to certain sites which have been blacklisted or which have been deemed to be unsuitable.

(xi) RIAM users are asked to avoid usage that would adversely affect productivity or consumes excessive network resources.

(xii) Service users should not violate copyright laws when downloading music files or images from the Internet, or infringe intellectual property rights including trademark, patent, design and/or moral rights in the process.

(xiii) Service users must not use the RIAM Internet connections (business and/or student networks) to scan or attack other individuals/devices/organisations. Service users must not use RIAM computers to make unauthorised entry into any other computer or network, or participate in unauthorised activity which results in heavy network traffic and thereby interrupts the legitimate use by others of RIAM resources.

(xiv) Service users must not disrupt or interfere with other computers or network users, services, or equipment. Intentional disruption of the operation of computer systems and networks is a crime under the Computer Misuse legislation.

(xv) Copyright and intellectual property rights of information service users may encounter on the Internet must be respected at all times. This may require obtaining appropriate permission to make use of information and the giving of proper credit to the source of the information used for RIAM’s purposes.

(xvi) Service users must not breach any other laws or ethical standards using RIAM ICT resources and internet facilities.

(xvii) Material in which RIAM has a proprietary interest – such as software, documentation or other internal or confidential information – must not be transmitted, sold or otherwise transferred to any outside party, except in pursuance of RIAM’s legitimate business interests. Any departure from this policy requires the written authorisation of the RIAM Secretary.

6.1.5 Social Media Usage

(i) Service users must not post messages on newsgroups or chat areas that are likely to be considered abusive, offensive, defamatory or inflammatory by others.

(ii) Service users are asked to refrain from posting, transferring, downloading, viewing or linking to material that is illegal, offensive, abusive, obscene, defamatory or threatening. Service users must not obtain/download, store and/or distribute text or images which contain any materials prohibited by law, or material of an inappropriate or offensive nature including pornographic, racist or extreme political nature, or which incites violence, hatred or any illegal activity.

(iii) Misuse of internet facilities and services is prohibited. RIAM's internet facilities, communication tools, such as email, social media (Facebook, WhatsApp, Twitter/X, etc.) or other means never be used:

- for personal gain or profit;
- to represent one's identity as someone else's;
- to obtain personal information on staff, students and/or external parties without their express permission;
- to post or download messages that will reflect poorly on RIAM's name and professional reputation;
- to advertise, or otherwise promote, unauthorised or illegal activities;
- to promote or engage in any business activity that is in competition with the RIAM's business activities;
- to process the personal data of any person in a manner inconsistent with the data protection legislation requirements;
- to process or disseminate any material that could be deemed to be threatening, harassing, illegal, obscene, defamatory, slanderous, or hostile towards any individual or entity.

The following applies to the use of social media whether during office hours or otherwise and regardless of whether the social media is accessed using RIAM ICT facilities and equipment or equipment belonging to members of staff or some other party:

- Staff, Students and external parties should also avoid social media communications that might be misconstrued in a way that could damage RIAM's interests and reputation, even indirectly.
- Staff, Students and external parties are personally responsible for what they communicate in social media.
- If your affiliation as a staff member, student or external party of RIAM is disclosed, it must be clearly stated that the views presented do not represent those of RIAM. For example, you could state, "the views in this posting do not represent the views of RIAM".

- Avoid posting comments about sensitive work-related topics. Even if you make it clear that your views on such topics do not represent those of the Institute, your comments could still damage RIAM's reputation.

- Strive for accuracy in any material you post online.

- If you see content in social media that disparages or reflects poorly on RIAM or staff, students or external parties of RIAM, you should contact your line manager.

- Do not post information including personal information related to RIAM.

- Staff, Students and external parties should avoid misappropriating or infringing the intellectual property of companies and/or individuals, which can create liability for RIAM as well as the individual author. Service users should familiarise themselves with current Irish and EU copyright law (ref section 9 below).

- Staff, Students and external parties should not use RIAM logos, brand names, slogans or trademarks without prior approval.

- Staff, Students and external parties should not post any of RIAM's confidential or proprietary information without prior written permission.

- Staff, Students and external parties should not use material or ideas without citing appropriate reference sources or acknowledging copyright accurately (ref Plagiarism Policy and Procedure).

- Non-compliance with the general principles and conditions of this internet and social media policy may lead to disciplinary action (for staff, up to and including dismissal).

6.1.6 Mobile Devices

(i) Mobile devices such as smartphone, laptops and tablet computers represent a significant risk to information security as they can easily become a conduit for unauthorised access to RIAM's data and ICT infrastructure, which could lead ultimately to data leakage and system infection.

(ii) Devices must be configured with a secure password.

(iii) With the exception of those devices managed by RIAM ICT, all other devices are not allowed to be connected directly to the internal business network.

(iv) RIAM is committed to meeting its legal and duty of care obligations while at the same time providing a flexible environment to allow the use of non-RIAM owned or issued devices to access corporate systems and store RIAM information (ref Bring Your Own Device and Use of Facilities Policy).

6.1.7 Software Protection

(i) All users must respect the legal protections to data and software provided by copyright and license agreements. Only licensed software products should be installed on RIAM information systems and services to ensure that the RIAM conforms to all copyright laws. Users are not permitted to load any unauthorised and/or unlicensed software onto RIAM Resources.

(ii) The licensed products should only be installed by systems administrators.
(iii) The ICT Manager will audit installed software applications from time to time and may remove unauthorised or unlicensed software from information systems.

(iv) Unauthorised copying of software or the use of unauthorised products by service users may be grounds for disciplinary action, up to and including dismissal (for staff), and where appropriate, legal proceedings.

6.1.8 Use of Artificial Intelligence

(i) Artificial intelligence (AI) represents a branch of computer science that aims to create machines capable of performing tasks that typically require human intelligence. These tasks include learning from experience (machine learning), understanding natural language, recognizing patterns, solving problems, and making decisions. AI works by simulating human intelligence through the use of algorithms, data, and computational power. Unlike traditional computer programs that follow predetermined instructions, AI systems can learn and adapt from data, allowing them to improve their performance over time. This ability to learn and evolve is a key characteristic that sets AI apart from conventional computing. RIAM policy on the use of AI by staff and students in the institution will be formulated after the benefits and consequences of AI have been fully assessed by the authorities.

6.2 Custodianship and Asset Protection

6.2.1 RIAM retains overall responsibility and ownership for all the institution’s records, information and ICT assets.

6.2.2 Individuals and departments are tasked, as custodians, with creating, maintaining and protecting these assets. Custodians are to be briefed on safeguarding of assigned assets.

6.2.3 Custodians of ICT assets are responsible for the protection, integrity and availability of those assets and for putting the appropriate controls and procedures in place in line with requirements set out in this policy.

6.2.4 Tangible/ physical assets are to be located in appropriately secure physical locations and securely stored away before closing.

6.2.5 Custodians of ICT assets are responsible for ensuring no assets under their assignment are removed from premises.

6.2.6 Controls and processes will be put in place to ensure assets are accurate, up-to-date and protected from unauthorised modification.

6.3 Access Control, Identity, Authentication and Password Control

6.3.1 Access controls for all RIAM ICT systems will be maintained at appropriate levels by ongoing proactive management.

6.3.2 Access to all RIAM ICT systems will use a secure log on process i.e. HEAnet's Edugate federated single sign on identity management system.

6.3.3 Staff will only be given access to those information systems that they are required to utilise in order to fulfil their duties. Line Managers must ensure that their staff have been adequately trained so that the integrity of the information systems can be maintained.

6.3.4 Where new staff members require access to the RIAM business network they will be assigned a network account in the Active Directory and a faculty licence for Office 365 by the system administrator.

6.3.5 New third level students will be given access to devices connected to the student network and allocated a student licence for Office 365.

6.3.6 Password for all RIAM systems are subject to the following rules:

(i) No passwords are to be spoken, written, emailed, hinted at, shared, or in any way known to anyone other than the user involved. This includes teachers, supervisors and personal assistants.

(ii) No passwords are to be shared in order to "cover" for someone out of the office. Contact the ICT Manager at tech@riam.ie to request a temporary account if there are resources that need to be accessed.

(iii) Service users should not use proper names, address details, dates of birth, or any term that could easily be guessed by someone who is familiar with them.

(iv) Passwords should not to be written down, displayed or concealed near workstations.

(v) Service users will be responsible for all activity conducted using their login details.

6.3.7 Service users are advised to select a long unique passphrase that is easy to remember, has not been in precious password breaches, found in a dictionary, repetitive or sequential (e.g. 'uuuuuuuu', '1234abcd'), or context-specific (e.g. derivatives of the name or service or the username).

6.3.8 If a password manager is chosen it is recommended that service users create unique passphrases/passwords for all their accounts and avoid using password managers that allow the recovery of the master password.

6.3.9 Service users should generate random, complex answers for online security questions.

6.3.10 Service users should change their passwords at regular intervals (every three months or whenever prompted by the system).

6.3.11 A Self-Service Password Reset (SSPR) facility is available to staff and third level students.

6.3.12 Service users should ensure that no equipment is left unattended in open to public traffic areas. Unattended equipment must have appropriate protection in place, such as automatic lock out screen. Users must terminate active sessions once task is complete or by using a password protected screen saver prior to leaving the work station. Users should also consider manually locking out of their workstations by pressing the Windows key and the letter 'l' simultaneously.

6.3.13 It is the policy of RIAM not to issue generic user accounts. Existing generic user accounts are to be reviewed and discontinued if no named user can be identified.

6.3.14 Whenever there is a change in business need, a user changes their role, or a user leaves RIAM, service user access rights will be adjusted appropriately and in a timely manner by the system administrator.

6.3.15 Where systems store data classified as 'confidential' or 'strictly confidential' additional steps will be taken to prevent unauthorised access. These may include encrypting the data and reviewing audit logs to monitor access to this data.

6.3.16 Multi-factor authentication (MFA) is enabled on all RIAM staff and third level student accounts.

6.3.17 Two-factor authentication will be employed where non-RIAM users are allowed to access RIAM online services.

6.4 Physical Security

6.4.1 RIAM servers and storage area network (SAN) switches, routers, firewalls, etc. are located in secure, temperature-controlled Communication Rooms (ref Comms Room Policy).

6.4.2 Computer equipment is installed in office environments and should be locked when unattended.

6.4.3 Equipment that supports critical business activities are physically protected from security threats and environmental hazards to reduce the risk of damage, interference and unauthorised access.

6.4.4 Only authorised persons are admitted access to these areas and appropriate entry controls are implemented (e.g. intruder alarm system, CCTV cameras).

6.4.5 Cables carrying data or supporting information services are protected by using conduit, by avoiding routes through public areas and installing them underground where feasible.

6.4.6 Equipment is correctly maintained to ensure its continued availability and integrity and servicing is only performed by experienced personnel.

6.4.7 All data is completely erased from equipment and storage media prior to disposal.

6.4.8 Remote service users must abide by the following guidelines:

(i) personal computers should not be used for business activities if virus controls are not in place;

(ii) when travelling, equipment (and media) should not be left unattended in public places;

(iii) portable devices should be carried as hand luggage when travelling;

(iv) time-out protection should be applied;

(v) all mobile devices should have an appropriate form of access protection (e.g. passwords or encryption) applied to prevent unauthorised access to their contents;

(vi) passwords or other access tokens for RIAM systems should never be stored on mobile devices in a plain text or image format which could lead to compromise or unauthorised access;

(vii) security risks should be assessed and appropriate measures put into practice.

(ref Flexible and Remote Working Policy and Procedure)

6.4.9 Service users must be aware of types of Physical Security types of breaches, such as tailgating, breach of clear screen/ clear desk guidelines and not limited to but including unauthorised access into secured areas (ref Clear Desk and Screen Policy).

6.4.10 Physical security incidents can be defined as issues that affect the physical barriers and control procedures that are implemented to act as preventive measures and countermeasures against threats to resources and sensitive information.

(i) If a suspected physical security incident is identified the incident should be reported immediately giving as much detail as possible.

(ii) If the incident is clearly a significant breach of security the RIAM Secretary should be consulted.

6.5 Maintenance and Technical Vulnerability

Patch Management

As part of the agreement between RIAM and managed service providers computer systems attached to the network and RIAM workstations and laptops must be updated accurately and timely with security protection mechanisms (patches) for known vulnerabilities and exploits to reduce or eliminate these vulnerabilities with limited impact to the business.

6.5.1 All security patches will be applied as soon as possible after their release and a log of the status of all patches is recorded.

6.5.2 Monitoring software is used to check each device on the network and alert the system administrator when patches are due to be downloaded and installed.

Remote Access to Systems

6.5.3 Remote access is allowed via secure connections only.

6.5.4 VPN facilities are provided to RIAM staff for the purpose of remote working and systems administration.

6.5.5 VPN connections are provided to authorised personnel who support applications remotely.

Anti-Virus Security

6.5.6 RIAM will provide MS Defender for Endpoints as part of the A5 M365 license to all members of staff and third level students.

6.5.7 Service users must ensure that they are running adequate and up-to-date anti-virus software at all times.

6.5.8 If any service user suspects that his/her machine has been infected with a virus, a complete virus scan should be performed.

6.5.9 If a machine is found to be behaving abnormally due to a possible viral infection this device will be disconnected from the network until deemed safe.

6.5.10 If a serious widespread virus attack occurs emergency procedures will be invoked which may include shutting down systems and the network. This will ensure immediate action by RIAM staff and students to ensure the safety of RIAM information resources through viral scan and disconnection.

6.6 Change Management and Testing

6.6.1 There is strict control over the implementation of changes to software installations.

6.6.2 Formal change control procedures are followed to ensure that security is not compromised and that formal agreement and approval for any change is obtained:

(i) Authorisation of request for change.

(ii) Risk assessment of change.

(iii) User acceptance testing.

(iv) Relevant management sign-off.

(v) Information security sign-off.

(vi) Rollback procedures in the event that the new release failed.

(vii) Documentation of above steps.

6.7 Confidentiality and Privacy

6.7.1 RIAM and all RIAM staff, third level students and stakeholders are obliged to respect the rights of individuals and to protect confidential data. Attention is drawn in particular to the:

(i) Code of Business Practice for Employees and Student Code of Conduct documents.

(ii) Breaches of the Code of Business Practice for Employees and Student Code of Conduct.

(iii) Legal requirements under the Data Protection Act 2018 and General Data Protection Regulation (GDPR).

6.8 Business Continuity

6.8.1 Continuity of operations, plans and arrangements ensure that there are mechanisms in place to maintain, or quickly resume, essential services and operations within RIAM in the event of a catastrophic event (e.g. fire, flooding etc.) that would result in disruption of normal activities and services.

6.8.2 A disaster plan has been devised outlining the disaster recovery management procedures and processes to ensure the efficient and effective resumption of vital RIAM functions in the event of an unscheduled interruption:

(i) review of RIAM systems, physical locations and current backup strategy;

(ii) actions to be taken by members of staff in the event of systems failure or data loss;

(iii) ongoing systems backup strategy;

(iv) systems continuity testing procedures;

(v) immediate actions to be taken.

6.8.3 Procedures for procuring replacement hardware or expanding web services have been agreed if disaster strikes.

6.8.4 The RIAM cloud infrastructure is robust and reliable. An image of the virtual machines will be used to replicate the existing MS Azure infrastructure and controls as part of the recovery strategy.

6.8.5 All files stored in MS Azure cloud web services will be secure against attack.

6.8.6 There is a nightly backup taken of all essential files stored in M365 faculty and third level student accounts and on virtual machines in the RIAM Azure tenancy. Backups are stored in the cloud and files are replicated to an external storage facility in another region in order to have reliable backups in the event of a physical disaster such as fire or flooding. If user files are deleted or become corrupt the original files can be restored from these backups.

6.8.7 All RIAM staff must be prepared for a disaster event in which ICT equipment or data is destroyed by ensuring that they have taken a backup of all important data stored on equipment assigned to them, or that they have saved a copy of all of these files to OneDrive or SharePoint which are backed up each night.

6.8.8 RIAM third level students are permitted to store files that they created in class in their own individual OneDrive accounts. Students are assigned secure RIAM network login details to allow them to access computers in the Music Technology Laboratory and the Library for this purpose. Students are also advised to save their own work to portable storage devices on a regular basis.

6.8.9 RIAM employees should not transfer or backup RIAM data to portable storage devices.

6.9 HEAnet Code of Behaviour

6.9.1 HEAnet is Ireland's National Education and Research Network, providing internet connectivity and associated ICT services to education and research and supplies enabling and enhancing services for RIAM in the pursuance of their official activities of instruction, research and development, and associated academic activities, and for administration in direct support of such use. RIAM has agreed that its staff and third level students will abide by HEAnet’s code of behaviour.

6.9.2 According to this code of behaviour it is not permitted to use HEAnet services for any activity which purposely:

(i) seeks to gain unauthorised access to the resources of member organisations;

(ii) adversely affects the operation of HEAnet services or jeopardises the use or performance for other users;

(iii) wastes resources (people, capacity, computer);

(iv) destroys the integrity of computer-based information;

(v) compromises the privacy of users;

(vi) creates or transmits (other than for properly supervised and lawful research purposes) any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;

(vii) creates or transmits defamatory material;

(viii) transmits material in such a way as to infringe the copyright of another person or organisation;

(ix) transmits unsolicited commercial or advertising material;

(x) causes offence or discriminates on grounds of race, creed or sex. In particular, compliance with the Employment Equality Act 1998, Equal Status Act 2000 and the Equality Act 2004 is required – including any amendments to said acts;

(xi) conflicts with practices as laid down from time to time by the Board contravenes the law of the State (in particular, but not exclusively, the Data Protection Act 2018 and the Criminal Damages Act (1991)).

7. Procedures and Compliance

7.1 Compliance with this policy is mandatory and will be deemed to be part of the contract of employment for staff and third parties. Each user must understand his/her role and responsibilities regarding information security issues, and protecting RIAM's information assets.

7.2 Failure to adhere and comply with this ICT policy that results in the compromise of RIAM information confidentiality, integrity and/or availability may result in disciplinary action (for staff, up to and including dismissal) and possible prosecution under applicable legislation.

7.3 Any compromise or suspected compromise of this policy must be reported as specified in the Code of Conduct.

7.4 An ICT security Incident is defined as any activity that harms or represents a serious threat to the whole or part of RIAM's computer, telephone and network-based resources such that there is an absence of service, inhibition of functioning systems. This includes unauthorised access or changes to, or theft of hardware, firmware, software or data, or a crime or natural disaster that destroys access to or control of these resources. It also includes the use of ICT resources in a manner that constitutes a criminal act.

7.5 Users of information systems are required to note and report any observed or suspected security weaknesses in, or threats to, systems and services. Such weaknesses or threats should be treated as security incidents, and be reported promptly to the ICT Manager.

7.6 All ICT incidents must be reported without delay to the ICT Manager, to the Line Manager or Senior Management as appropriate.

7.7 Evidence relating to a suspected data security breach should be recorded and notified to the Data Controller and Data Protection Officer and appropriate remedial action taken immediately (ref Data Protection Policy).

7.8 Security incidents reported to the ICT Manager will be subject to appropriate internal procedures. Where it is deemed appropriate files may be deleted to minimise the risk of propagation or the network may be isolated to maintain its integrity.

7.9 All employees should be made aware that evidence of information security incidents may be formally recorded and retained.

7.10 Wherever possible, the RIAM will undertake to prevent incidents by monitoring and scanning its own network for anomalies, and developing clear protection procedures for the configuration of its ICT resources.

7.12 Service users are asked to display common sense and courtesy when handling emails, as any action that adversely affects ICT systems will impact upon the business/educational needs of all service users in RIAM.

7.13 RIAM users must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. RIAM reserves the right to block or monitor access to such material.

7.14 These procedures will be reviewed periodically to adjust processes, identify new risks and remediation methods.

8. Responsibility

8.1 The responsibility for protecting ICT systems and information rests with all staff, third level students and third parties who use or have involvement with the systems. Both the RIAM ICT user community and ICT services have responsibilities to ensure compliance with this policy.

8.2 The RIAM Senior Management team has overall responsibility for the RIAM ICT policy to protect the assets of the institution. Appropriate procedures must be in place together with management, monitoring and review processes to ensure that policies are implemented, adhered to and kept up-to-date.

8.3 The ICT Steering Committee oversees the ICT infrastructure, database systems and assets, makes recommendations to Senior Management, reports on ICT security matters and ensures that policies are implemented in order to avoid breaches of legal, statutory, regulatory, contract or privacy obligations.

8.4 The ICT Manager plays a key role in the implementation of the ICT Policy and has responsibility for monitoring the RIAM network infrastructure, including all hardware and communication links, reporting any audit issues that may be identified in relation to these items, and providing advice and assistance to end users.

9. Legislation and Regulation

9.1 Copyright and Related Rights Act 2000, 2004 and 2007.

9.2 Data Protection Act 2018.

9.3 Child Trafficking and Pornography Act 1998.

9.4 Child Trafficking and Pornography (Amendment) Act 2004.

9.5 Criminal Damages Act 1991.

9.6 Defamation Act 2009.

9.7 Employment Equality Act 1998.

9.8 Equal Status Act 2000.

9.9 Equality Act 2004.

9.10 Prohibition of Incitement to Hatred Act 1989.

9.11 Qualifications and Quality Assurance (Education and Training) Act 2012.

9.12 Standards and Guidelines for Quality Assurance in the European Higher Education Area (2005).

9.13 Code of Practice for Provision of Education and Training to International Learners (2015).

9.14 National Framework of Qualifications (NFQ).

9.15 General Data Protection Regulation (GDPR) 2018.

9.16 Data Protection Commission - Rules for Electronic and Direct Marketing

10. Related Documents

10.1 Bring Your Own Device and Use of Facilities Policy.

10.2 Flexible and Remote Working Policy and Procedure.

10.3 Clear Desk and Screen Policy.

10.4 Code of Business Practice for Employees.

10.5 Comms Room Policy.

10.6 Data Protection Policy.

10.7 Plagiarism Policy and Procedure.

10.8 Records Retention Policy.

10.9 Staff Disciplinary Policy.

10.10 Staff Grievance and Mediation Policy.

10.11 Student Code of Conduct Policy.

11. Review

11.1 This policy will be reviewed on a three-year cycle, or as required to take into account changes in the law and the experience of the policy in practice.

12. Document Control

Approved by Board of Studies 25th November 2016.
Revision 1 approved by Board of Studies 10th March 2017.
Revision 2 approved.
Revision 3 approved by Trinity Academic Council 13th May 2020.
Revision 4 approved by RIAM Governing Body 11th July 2024.

Next review: Academic year 2027/28.